

Guía de Entrevista para Expertos: Gobernanza y Seguridad de IA

I. Protocolo de Apertura

- **Presentación**
Explicación del objetivo de la investigación (Lineamientos estratégicos para el uso de Gemini en Acciones & Valores).
- **Consentimiento**
Lectura y firma del consentimiento informado para grabación y transcripción con fines académicos.
- **Perfil del Experto**
Cargo, años en la firma y relación directa con la gestión de riesgo tecnológico.

II. Eje Temático 1: Gobernanza de la IA (NTC-ISO/IEC 42001:2023)

Objetivo: Entender cómo se integra la IA en la estructura de control actual.

1. ¿Cómo ha sido el proceso de integración de herramientas como Gemini en la estrategia de transformación digital de la firma?
2. Desde la perspectiva de la norma **NTC-ISO/IEC 42001:2023**, ¿quiénes deberían ser los responsables directos de supervisar el ciclo de vida de los datos en modelos de IA dentro de la organización?
3. ¿Qué tan preparados están los comités de riesgos actuales para evaluar los impactos éticos y de privacidad de la IA generativa?

III. Eje Temático 2: Cumplimiento Normativo (SFC y Ley 1581)

Objetivo: Evaluar la alineación con los requerimientos legales del sector bursátil.

4. ¿Qué desafíos específicos presenta la **Circular Externa 007 de 2023** de la SFC frente al uso de modelos de lenguaje externos?
5. En el marco de la **Ley 1581 de 2012**, ¿qué protocolos de anonimización considera usted indispensables antes de que un analista interactúe con una IA pública?
6. ¿De qué manera el uso de Gemini podría afectar el cumplimiento del **SARO** (Riesgo Operativo) en las operaciones de mercado?

IV. Eje Temático 3: Gestión del Riesgo Tecnológico (Exfiltración y Shadow AI)

Objetivo: Identificar brechas no documentadas en el flujo de datos.

7. ¿Cuáles considera que son los puntos ciegos o "Shadow AI" (uso no autorizado) que podrían existir actualmente entre los analistas de la firma?
8. En un escenario de **exfiltración de datos** a través de un prompt, ¿cuál sería el impacto inmediato en el activo reputacional de Acciones & Valores?
9. ¿Cómo diferencia la firma actualmente entre una fuga de información accidental y una exfiltración deliberada de propiedad intelectual mediante IA?

V. Eje Temático 4: Controles de Seguridad (Muros de Contención: DLP y Firewall)

Objetivo: Obtener detalles técnicos sobre las barreras de defensa.

10. ¿Qué tan efectivas son las reglas actuales de **DLP (Data Loss Prevention)** para detectar y bloquear información financiera sensible en el tráfico hacia servidores de IA?
11. ¿Cuál es su postura técnica sobre el uso de instancias **Gemini Enterprise** frente a la implementación de un firewall de IA de desarrollo propio?
12. ¿Qué técnicas de **enmascaramiento de datos** o seudonimización resultan más viables para los procesos de trading y remesas de la firma?

VI. Protocolo de Cierre

- **Recomendaciones:** Según su experiencia, ¿cuál debería ser el primer lineamiento que la firma debe oficializar para el uso seguro de IA?
- **Comentarios finales:** Espacio libre para observaciones que no se hayan cubierto en los ejes temáticos.
- **Agradecimiento:** Cierre formal de la sesión.

Consideraciones Técnicas para el Analista:

- **Precisión:** El entrevistador debe estar familiarizado con términos como *prompt engineering*, *tokens* y *fine-tuning* para profundizar en las respuestas del experto.
- **Duración:** Si la entrevista se extiende más allá de los 60 minutos, prioriza el Eje Temático 4 sobre controles técnicos, ya que es el "corazón" de tu propuesta de seguridad.

